UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,963	06/27/2001	Dwip N. Banerjee	AUS920010369US1	3820

7590 04/19/2005

Kelly K. Kordzik
5400 Renaissance Tower
1201 Elm Street
Dallas, TX 75270

EXAMINER	
SHAH, CHIRAG G	

ART UNIT	PAPER NUMBER
2664	

DATE MAILED: 04/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/892,963	BANERJEE ET AL.	
	Examiner	Art Unit	
	Chirag G Shah	2664	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 6/27/01.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-44 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-4, 7, 10-13, 16-19, 22, 25-28, 31-34, 37, and 40-42 is/are rejected.

7)☒ Claim(s) 5-6, 8-9, 14-15, 29-21, 23-24, 29-30, 35-36, 38-39, and 43-44 is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 6/27/01 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 6/27/01.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: Please Delete the Attorney Docket Numbers on page 1, line 5 and page 14, lines 12-13 and replace with appropriate Serial Number or Patent Number.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-4, 7, 10, 12-13, 31-34, 37 and 41-42 rejected under 35 U.S.C. 103(a) as being unpatentable over Goldstone (U.S. Pub. No. 2002/0101819) in view of Shanklin et al. (U.S. Pub. No. 2002/0133586).

Regarding claim 1, Goldstone discloses in **claims 16, 22 and figure 4** of a method for preventing at least in part a server overload comprising the steps of:

Goldstone discloses a destination server **[target web server 10, fig. 4] detects bandwidth congestion/server overload condition [as in claim 16 and 22]** based on **receiving excessive packet requests from attacking client [as disclosed 0038 and 0042]**;

Goldstone discloses of sending a request to one or more of one or more routers **[server 10 of fig. 4, informing a origin site router 30 of figure 4]** connected to said server having a

privilege relationship with said server **[as disclosed in paragraph 0041, Site Router 30 routes the request packet to the target server directly or through a (secure logic) firewall]**, wherein said request is a request to block IP address of the router that corresponds to sending excessive packet requests, and

Goldstone fails to explicitly disclose that overload due to bandwidth congestion caused by sending numerous unauthorized packets to the server corresponds to excessive number of packets exceeding a predetermined limit and the router blocking the excessive number of packets detected for a first period of time.

Shanklin teaches of preventing unauthorized access to a network. Shanklin discloses in paragraph **0064** of a **set predetermined limit/threshold (predetermined limit)** for data packet count, which represents the maximum number of packets per sample time, and if the number of packet from any one source exceeds the data packet threshold value (creating a bandwidth congestion) during the pre-determined sample time, all the packets from that source will be denied (blocked). Shanklin discloses in **0014** of activating an IDS (Intrusion Detection System) on a router, Shanklin discloses in **0012 that if the number of packets from any one source exceeds the data packet count threshold during the sample period, all data packets from that source to a specific destination are denied access (blocked) to the network port**.

Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Goldstone to include blocking the excessive number of packets detected for a first period of time as taught by Shanklin. **One is motivated as disclosed in paragraphs 0020 as such in order to provide greater flexibility and greater accuracy in identifying attack source/data packets.**

Regarding claim 31, Goldstone discloses in **figures 1 and 4 of a system**, comprising:

a server **[target server 50, figure 4]**;

one or more routers **[site router 30, figure 4]** coupled to said server **[target web server 10, figure 4]**; and

one or more clients **[client attacking site 60, figure 4]** coupled to said server **[target web server 10, figure 4]** by way of an Internet **[figure 1]**;

wherein one or more of said one or more routers **[site router 30, figure 4]** coupled to said server **[target web server 10]** having a privilege relationship **[as disclosed in paragraph 0041, Site Router 30 routes the request packet to the target server directly or through a (secure logic) firewall]** with said server **[target web server 10, fig. 4].**

Goldstone **discloses in claims 16 and 22**, that the destination site server detects the bandwidth congestion/server overload (which is caused by client sending bogus packet requests exceeding server's capacity, causing the server to detect bandwidth congestion as disclosed in paragraphs **0038 and 0042**). Goldstone further discloses in claim 16, the destination server 10 informs the site router 30, the attacking address corresponding to the attacking client site from where the bandwidth (exceeding packet) congestion originated. **Thereafter, as disclosed in paragraph 0042 and claim 17, the site router receiving (message) the attacking client's IP address from the destination site server, the router, then, prevents/blocks the attacking address (router blocks the client's address from where the bogus packet requests exceeding server's capacity were sent from) corresponding to the attacking site form being used to gain access to the Server via Internet or other WAN.**

Goldstone as disclosed in claim 16 and 22, as mention above site router receives from the server, a message informing of a bandwidth congestion/server overload and an address corresponding to attacking client site from where the congestion originated. Router then blocks attacker IP address, however fails to explicitly disclose of the router blocking the excessive number of packets detected for a first period of time.

Shanklin teaches of preventing unauthorized access to a network. Shanklin discloses in 0014 of activating an IDS (Intrusion Detection System) on a router, Shanklin discloses in **0012 and 0064** that if the number of packets from any one source exceeds the data packet count threshold during the sample period, all data packets from that source to a specific destination are denied access to the network port.

Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Goldstone to include blocking the excessive number of packets detected for a first period of time as taught by Shanklin. **One is motivated as disclosed in paragraphs 0020 as such in order to provide greater flexibility and greater accuracy in identifying attack source/data packets.**

Regarding claims 2 and 32, Goldstone **discloses in paragraphs 0042-0043** of further comprising the step of:

propagating said request to block said excessive number of packets **(bogus packet request, see 0042)** to one or more neighboring routers **(ISP router 50, see 0042)** by one or more of said one or more routers **(site router 30, see 0042)** having said privilege relationship with said

server **[Based on figure 4, the site router 30 has a secure server access with web server 10 via firewall, as disclosed in 0042-0043, the site router 30 automatically propagates the request to block to a neighboring ISP router 50, which uses its access list to prevent any further bogus packet request]** as claim .

Regarding claims 3 and 33, Goldstone **discloses in paragraph 0042** of further comprising the step of: determining whether to block said excessive number of packets by said one or more neighboring routers **[as disclosed in paragraph 0042, the neighboring ISP router 50 upon receiving the attacking client's IP address, determines to block using the access list, the attacking client's IP address from further sending bogus packet request to the server]** as claim.

Regarding claims 4 and 34, Goldstone discloses in 0042-0043 of neighboring router 50 blocking attacking client's IP address preventing the client from transmitting bogus packet requests to the server.

Goldstone fails to disclose wherein each of said one or more neighboring routers includes a configuration file, wherein said configuration file comprises information indicating whether to honor said request to block said excessive number of packets.

Shanklin discloses in **paragraphs 0012-0014**, of a **router including a configuration file that controls the parameters of operation**. In operation, if the number of packets from any one source exceeds the data packet count threshold during the sample period, all data packets from that source to a specific destination are denied/blocked access to the network port. Thus, clearly

suggesting that the configuration file includes control information with respect to blocking the data packets if the source exceeds the data packet count threshold.

Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Goldstone to include a configuration file within a router for controlling the blocking the excessive number of packets as taught by Shanklin. **One is motivated as such in order to provide the parameter of operation enabling the execution of denial conditions such as blocking of excess data packet upon exceeding threshold,** *see Shanklin 0012.*

Regarding claim 7 and 37, Goldstone discloses in **paragraphs 0042-0044** of further comprising the steps of: determining whether to propagate the request by said one or more neighboring routers **[as disclosed in paragraphs 0042-0044, a router automatically communicates/propagates the IP address of the attacking client to the router that is physically closet to the attacker, this permits blocking of attacking client at the point closest to the entry to the Internet, thus diminishing the attacker's ability to find other routes of attack]** as claim.

Regarding claim 10, Goldstone discloses **0042-0043** wherein said request comprises one or more of an Internet Protocol address of a client **[as disclosed in 0042-0043, IP address of the attacking client is propagated to neighboring routers]** as claim.

Regarding claim 12 and 41, Goldstone disclosed a **site router 30, figure 4** coupled to said server **[target web server 10]** having a privilege relationship **[as disclosed in paragraph 0041, Site Router 30 routes the request packet to the target server directly or through a (secure logic) firewall]** with said server **[target web server 10, fig. 4].**

Goldstone fails to disclose explicitly of a router including a configuration file, wherein said configuration file comprises information indicating whether to honor said request to block said excessive number of packets.

Shanklin discloses in **paragraphs 0012-0014**, of a **router including a configuration file that controls the parameters of operation**. In operation, if the number of packets from any one source exceeds the data packet count threshold during the sample period, all data packets from that source to a specific destination are denied/blocked access to the network port. Thus, clearly suggesting that the configuration file includes control information with respect to blocking the data packets if the source exceeds the data packet count threshold.

Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Goldstone to include a configuration file within a router for controlling the blocking the excessive number of packets as taught by Shanklin. **One is motivated as such in order to provide the parameter of operation enabling the execution of denial conditions such as blocking of excess data packet upon exceeding threshold,** *see Shanklin 0012.*

Regarding claims 13 and 42, Goldstone disclosed a **site router 30, figure 4** coupled to said server **[target web server 10]** having a privilege relationship **[as disclosed in paragraph**

0041, Site Router 30 routes the request packet to the target server directly or through a (secure logic) firewall] with said server **[target web server 10, fig. 4].**

Goldstone fails to disclose explicitly of a router including a configuration file, wherein said configuration file comprises information indicating whether to honor said request to block said excessive number of packets for a first period of time.

Shanklin discloses in **paragraphs 0012-0014**, of a **router including a configuration file that controls the parameters of operation**. In operation, if the number of packets from any one source exceeds the data packet count threshold during the **sample period (first period of time)**, all data packets from that source to a specific destination are denied/blocked access to the network port. Thus, clearly suggesting that the configuration file includes control information with respect to blocking the data packets if the source exceeds the data packet count threshold.

Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Goldstone to include a configuration file within a router for controlling the blocking the excessive number of packets as taught by Shanklin. **One is motivated as such in order to provide the parameter of operation enabling the execution of denial conditions such as blocking of excess data packet upon exceeding threshold during a sample period of time,** *see Shanklin 0012.*

4. Claims 11 and 40 rejected under 35 U.S.C. 103(a) as being unpatentable over Goldstone in view of Shanklin as applied to claims 1-4, 7, 10, 12-13, 31-34, 37 and 41-42 above, and further in view of Lammle (CCNA Cisco Certified Network Associate, Second Edition).

Regarding claim 11 and 40, Goldstone in view of Shanklin discloses of a router connected to a server having a secure connection, including a configuration file.

Goldstone in view of Shanklin however fails to explicitly disclose that the configuration file comprises information indicating whether a particular router has said privilege relationship with said server.

Lammle discloses on page 327 of the major Cisco router components, including RAM where running-configuration files along with the Internetwork Operating System (IOS) reside. Lammle further discloses on pages 412-413 of commands that may be used on router to access the information for the router stored within the configuration file such as show ipx servers, show ipx interface, show ipx route etc... **Lammle specifically disclosed on page 413 that the show ipx servers command displays the content of the SAP table in the Cisco router. The output of the command on page 413 allows one to see all the accessible servers (logically connected) to the router. Thus, clearly establishing that configuration file stored logically secure server connections that a router may access via a particular route, port and address.**

Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Goldstone in view of Lammle to include a configuration file within a router storing for privilege relationship (logically accessible) with server as taught by Lammle. **One is motivated as such in order to provide information with respect to all the accessible servers for packet transfer and packet load management (Lammle 413, 414).**

5. Claims 16-19, 22, 25, and 27-28 rejected under 35 U.S.C. 103(a) as being unpatentable over Goldstone in view of Shanklin, and further in view of Smith (U.S. Patent No. 5,878,224).

Regarding claim 16, Goldstone discloses a system **[fig. 4]**, comprising:

a server **[web server 10, figure 4]**;

one or more routers **[site router 30, fig. 4]** coupled to said server **[web server 10, fig.4]**, wherein one or more of said one or more routers with a privilege relationship **[as disclosed in paragraph 0041, Site Router 30 routes the request packet to the target server directly or through a (secure logic) firewall]** with said server **[target web server 10, fig. 4].**

Goldstone further **discloses in claims 16 and 22**, that the destination site server detects the bandwidth congestion/server overload (which is caused by client sending bogus packet requests exceeding server's capacity, causing the server to detect bandwidth congestion as disclosed in paragraphs **0038 and 0042**). Goldstone further discloses **in claim 16**, the destination server 10 informs the site router 30, the attacking address corresponding to the attacking client site from where the bandwidth (exceeding packet) congestion originated. **Thereafter, as disclosed in paragraph 0042 and claim 17, the site router receiving (message) the attacking client's IP address from the destination site server, the router having the circuitry, then, prevents/blocks the attacking address (router blocks the client's address from where the bogus packet requests exceeding server's capacity were sent from) corresponding to the attacking site form being used to gain access to the Server via Internet or other WAN.**

one or more clients **[attacking site 60, fig. 4]** coupled to said server **[web server 10, fig. 4]** by way of an Internet **[as in fig 4]**; and

one or more neighboring routers **[ISP router 50, fig. 4]** coupled to said one or more clients **[attacking site 60, fig. 4]** configured to forward packets of data **[as disclosed in paragraph 0041]** from said one or more clients to said server **[web server 10, fig 4]**;

Goldstone discloses a destination server **[target web server 10, fig. 4] comprises** a processor [**as disclosed in claim 22**, the overload condition is detected by the server, establishing that server includes a processor];

a destination server **[target web server 10, fig. 4] detects bandwidth congestion/server overload condition [as in claim 16 and 22]** based on **receiving excessive packet requests from attacking client [as disclosed 0038 and 0042]**;

Goldstone discloses of sending a request to one or more of one or more routers **[server 10 of fig. 4, informing a origin site router 30 of figure 4]** connected to said server having a privilege relationship with said server **[as disclosed in paragraph 0041, Site Router 30 routes the request packet to the target server directly or through a (secure logic) firewall]**, wherein said request is a request to block IP address of the router that corresponds to sending excessive packet requests.

Goldstone fails to explicitly disclose that overload due to bandwidth congestion caused by sending numerous unauthorized packets to the server corresponds to excessive number of packets exceeding a predetermined limit and the router blocking the excessive number of packets detected for a first period of time.

Shanklin teaches of preventing unauthorized access to a network. Shanklin discloses in paragraph **0064** of a **set predetermined limit/threshold (predetermined limit)** for data packet count, which represents the maximum number of packets per sample time, and if the number of

packet from any one source exceeds the data packet threshold value (creating a bandwidth congestion) during the pre-determined sample time, all the packets from that source will be denied (blocked). Shanklin discloses in **0014** of activating an IDS (Intrusion Detection System) on a router, Shanklin discloses in **0012 that if the number of packets from any one source exceeds the data packet count threshold during the sample period, all data packets from that source to a specific destination are denied access (blocked) to the network port**.

Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Goldstone to include blocking the excessive number of packets detected for a first period of time as taught by Shanklin. **One is motivated as disclosed in paragraphs 0020 as such in order to provide greater flexibility and greater accuracy in identifying attack source/data packets.**

Goldstone in view of Shanklin fails to explicitly disclose that the server comprising a memory unit storing a computer program operable for preventing at least in part an overload of said server; a bus system coupling the processor to the memory unit, wherein the computer program comprises the programming steps of overload detection/prevention.

Smith discloses in the abstract of a system for preventing server overload. Smith further discloses in col. 4, lines 43-62 of a controller in a network server having mass storage, processing unit, and memory having overload control program implementing overload methods for preventing network server overload, internally coupled via a bus type system as depicted in figure 4.

Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Goldstone in view of Shanklin to include the server

having a memory unit for preventing an overload, coupled via a processor in a system as taught by Smith. **One is motivated as such in order to implement and execute via memory and processor the methods for preventing server overload based on messages received from a source initiating a network server transaction,** *see Smith col. 2, lines 50-61.*

Regarding claim 17, Goldstone **discloses in paragraphs 0042-0043** of further comprising the step of:

propagating said request to block said excessive number of packets **(bogus packet request, see 0042)** to one or more neighboring routers **(ISP router 50, see 0042)** by one or more of said one or more routers **(site router 30, see 0042)** having said privilege relationship with said server **[Based on figure 4, the site router 30 has a secure server access with web server 10 via firewall, as disclosed in 0042-0043, the site router 30 automatically propagates the request to block to a neighboring ISP router 50, which uses its access list to prevent any further bogus packet request]** as claim .

Regarding claim 18, Goldstone **discloses in paragraph 0042** of further comprising the step of: determining whether to block said excessive number of packets by said one or more neighboring routers **[as disclosed in paragraph 0042, the neighboring ISP router 50 upon receiving the attacking client's IP address, determines to block using the access list, the attacking client's IP address from further sending bogus packet request to the server]** as claim.

Regarding claim 19, Goldstone discloses in 0042-0043 of neighboring router 50 blocking attacking client's IP address preventing the client from transmitting bogus packet requests to the server.

Goldstone fails to disclose wherein each of said one or more neighboring routers includes a configuration file, wherein said configuration file comprises information indicating whether to honor said request to block said excessive number of packets.

Shanklin discloses in **paragraphs 0012-0014**, of a **router including a configuration file that controls the parameters of operation**. In operation, if the number of packets from any one source exceeds the data packet count threshold during the sample period, all data packets from that source to a specific destination are denied/blocked access to the network port. Thus, clearly suggesting that the configuration file includes control information with respect to blocking the data packets if the source exceeds the data packet count threshold.

Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Goldstone to include a configuration file within a router for controlling the blocking the excessive number of packets as taught by Shanklin. **One is motivated as such in order to provide the parameter of operation enabling the execution of denial conditions such as blocking of excess data packet upon exceeding threshold,** *see Shanklin 0012.*

Regarding claim 22, Goldstone discloses in **paragraphs 0042-0044** of further comprising the steps of: determining whether to propagate the request by said one or more neighboring routers **[as disclosed in paragraphs 0042-0044, a router automatically**

communicates/propagates the IP address of the attacking client to the router that is physically closet to the attacker, this permits blocking of attacking client at the point closest to the entry to the Internet, thus diminishing the attacker's ability to find other routes of attack] as claim.

Regarding claim 25, Goldstone discloses **0042-0043** wherein said request comprises one or more of an Internet Protocol address of a client **[as disclosed in 0042-0043, IP address of the attacking client is propagated to neighboring routers]** as claim.

Regarding claim 27, Goldstone disclosed a **site router 30, figure 4** coupled to said server **[target web server 10]** having a privilege relationship **[as disclosed in paragraph 0041, Site Router 30 routes the request packet to the target server directly or through a (secure logic) firewall]** with said server **[target web server 10, fig. 4].**

Goldstone fails to disclose explicitly of a router including a configuration file, wherein said configuration file comprises information indicating whether to honor said request to block said excessive number of packets.

Shanklin discloses in **paragraphs 0012-0014**, of a **router including a configuration file that controls the parameters of operation**. In operation, if the number of packets from any one source exceeds the data packet count threshold during the sample period, all data packets from that source to a specific destination are denied/blocked access to the network port. Thus, clearly suggesting that the configuration file includes control information with respect to blocking the data packets if the source exceeds the data packet count threshold.

Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Goldstone to include a configuration file within a router for controlling the blocking the excessive number of packets as taught by Shanklin. **One is motivated as such in order to provide the parameter of operation enabling the execution of denial conditions such as blocking of excess data packet upon exceeding threshold,** *see Shanklin 0012.*

Regarding claim 28, Goldstone disclosed a **site router 30, figure 4** coupled to said server **[target web server 10]** having a privilege relationship **[as disclosed in paragraph 0041, Site Router 30 routes the request packet to the target server directly or through a (secure logic) firewall]** with said server **[target web server 10, fig. 4].**

Goldstone fails to disclose explicitly of a router including a configuration file, wherein said configuration file comprises information indicating whether to honor said request to block said excessive number of packets for a first period of time.

Shanklin discloses in **paragraphs 0012-0014**, of a **router including a configuration file that controls the parameters of operation**. In operation, if the number of packets from any one source exceeds the data packet count threshold during the **sample period (first period of time)**, all data packets from that source to a specific destination are denied/blocked access to the network port. Thus, clearly suggesting that the configuration file includes control information with respect to blocking the data packets if the source exceeds the data packet count threshold. Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Goldstone to include a configuration file within a router for

controlling the blocking the excessive number of packets as taught by Shanklin. **One is motivated as such in order to provide the parameter of operation enabling the execution of denial conditions such as blocking of excess data packet upon exceeding threshold during a sample period of time,** *see Shanklin 0012.*

6. Claim 26 rejected under 35 U.S.C. 103(a) as being unpatentable over Goldstone and Shanklin in view of Smith as applied to claims 16-19, 22, 25 and 27-28 above, and further in view of Lammle (CCNA Cisco Certified Network Associate, Second Edition).

Regarding claim 26, Goldstone in view of Shanklin discloses of a router connected to a server having a secure connection, including a configuration file.

Goldstone in view of Shanklin however fails to explicitly disclose that the configuration file comprises information indicating whether a particular router has said privilege relationship with said server.

Lammle discloses on page 327 of the major Cisco router components, including RAM where running-configuration files along with the Internetwork Operating System (IOS) reside. Lammle further discloses on pages 412-413 of commands that may be used on router to access the information for the router stored within the configuration file such as show ipx servers, show ipx interface, show ipx route etc... **Lammle specifically disclosed on page 413 that the show ipx servers command displays the content of the SAP table in the Cisco router. The output of the command on page 413 allows one to see all the accessible servers (logically connected) to the router. Thus, clearly establishing that configuration file stored logically secure server connections that a router may access via a particular route, port and address.**

Therefore, it would have been obvious to one of ordinary skills in the art at the time of the invention to modify the teachings of Goldstone in view of Lammle to include a configuration file within a router storing for privilege relationship (logically accessible) with server as taught by Lammle. **One is motivated as such in order to provide information with respect to all the accessible servers for packet transfer and packet load management (Lammle 413, 414).**

Allowable Subject Matter

7. Claims 5-6, 8-9, 14-15, 20-21, 23-24, 29-30, 35-36, 38-39, and 43-44, objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, D.C. 20231

Or faxed to:

(703)305-3988, (for formal communications intended for entry)

Or:

(703)305-3988 (for informal or draft communications, please label "Proposed" or "DRAFT")

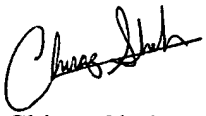
Hand-delivered responses should be brought to Crystal Park II, 2021 Crystal Drive, Arlington, VA., Sixth Floor (Receptionist).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chirag G Shah whose telephone number is 571-272-3144. The examiner can normally be reached on M-F 6:45 to 4:15, 2nd Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wellington Chin can be reached on 571-272-3134. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cgs
April 4, 2005



Chirag Shah
AU 2664